LUNTRY

luntry.ru

Вебинар

С чего начать защиту кластера Kubernetes?

Дмитрий Евдокимов

Founder&CTO Luntry

Андрей Ганюшкин

Коммерческий директор Luntry

whoami

- Основатель и технический директор Luntry
- Опыт в ИБ более 15 лет
- Специализация безопасность контейнеров и Kubernetes
- CFP 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
- Организатор конференции по безопасности контейнеров - БеКон
- Докладчик: BlackHat, HITB, ZeroNights, HackInParis, Confidence, SAS, OFFZONE, PHDays, Kazhackstan, DevOpsConf, DevOops, KuberConf, VK Kubernetes Conference, HighLoad++, БЕКОН и др.

LUNTRY
luntry.ru

whoami

- Коммерческий директор
- 10 лет в сфере безопасности, как на Российском, так и международном рынке
- Организатор конференции «БеКон» - первая в России

  конференция по БЕзопасности КОНтейнеров и контейнерных сред

luntry.ru

О компании Luntry

- Luntry – это Комплексная Защита на всем жизненном цикле контейнерных приложений и средств оркестрации на базе Kubernetes
- Продукт в реестре Минцифры
  - https://reestr.digital.gov.ru/reestr/1057835/
- В процессе получения сертификата ФСТЭК
  - Ориентировочно конец 2024

LUNTRY
luntry.ru

Функциональность Luntry

План вебинара

- Мировая практика
  - Threat matrix
  - NIST Cybersecurity Framework (CSF)
  - CIS Controls
  - CIS Kubernetes Benchmark
  - NIST SP 800-190
  - Risk8s Business
- Взгляд Luntry

Мировая практика

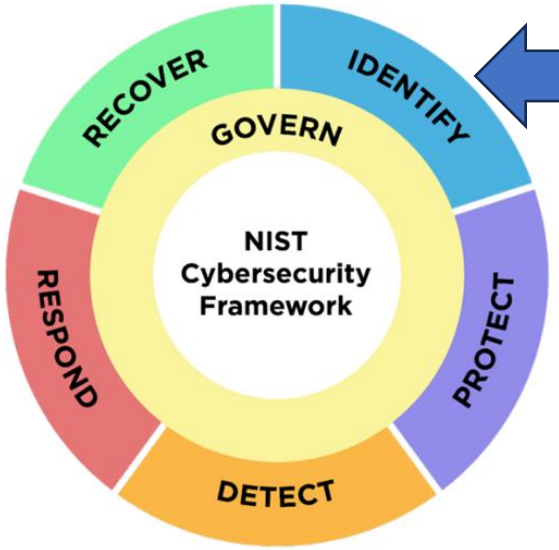
Threat matrix для Kubernetes от Microsoft

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Impact
Using cloud credentials	Exec into container	Backdoor container	Privileged container	Clear container logs	List K8S secrets	Access Kubernetes API server	Access cloud resources	Images from a private registry	Data destruction
Compromised image In registry	bash/cmd inside container	Writable hostPath mount	Cluster-admin binding	Delete K8S events	Mount service principal	Access Kubelet API	Container service account	Collecting data from pod	Resource hijacking
Kubeconfig file	New container	Kubernetes CronJob	hostPath mount	Pod / container name similarity	Container service account	Network mapping	Cluster internal networking		Denial of service
Application vulnerability	Application exploit (RCE)	Malicious admission controller	Access cloud resources	Connect from proxy server	Application credentials in configuration files	Exposed sensitive interfaces	Application credentials in configuration files		
Exposed sensitive interfaces	SSH server running inside container	Container service account			Access managed identity credentials	Instance Metadata API	Writable hostPath mount		
	Sidecar injection	Static pods			Malicious admission controller		CoreDNS poisoning		
							ARP poisoning and IP spoofing		

Источник

NIST Cybersecurity Framework (CSF)

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO



IDENTIFY (ID) — *The organization's current cybersecurity risks are understood.* Understanding the organization's assets (e.g., data, hardware, software, systems, facilities, services, people), suppliers, and related cybersecurity risks enables an organization to prioritize its efforts consistent with its risk management strategy and the mission needs identified under GOVERN. This Function also includes the identification of improvement opportunities for the organization's policies, plans, processes, procedures, and practices that support cybersecurity risk management to inform efforts under all six Functions.

CIS Controls

CIS Kubernetes Benchmark

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) “5.1 - Establish Secure Configurations” and (v8) '4.1 - Establish and Maintain a Secure Configuration Process” so individual recommendations will not be mapped to these safeguards.

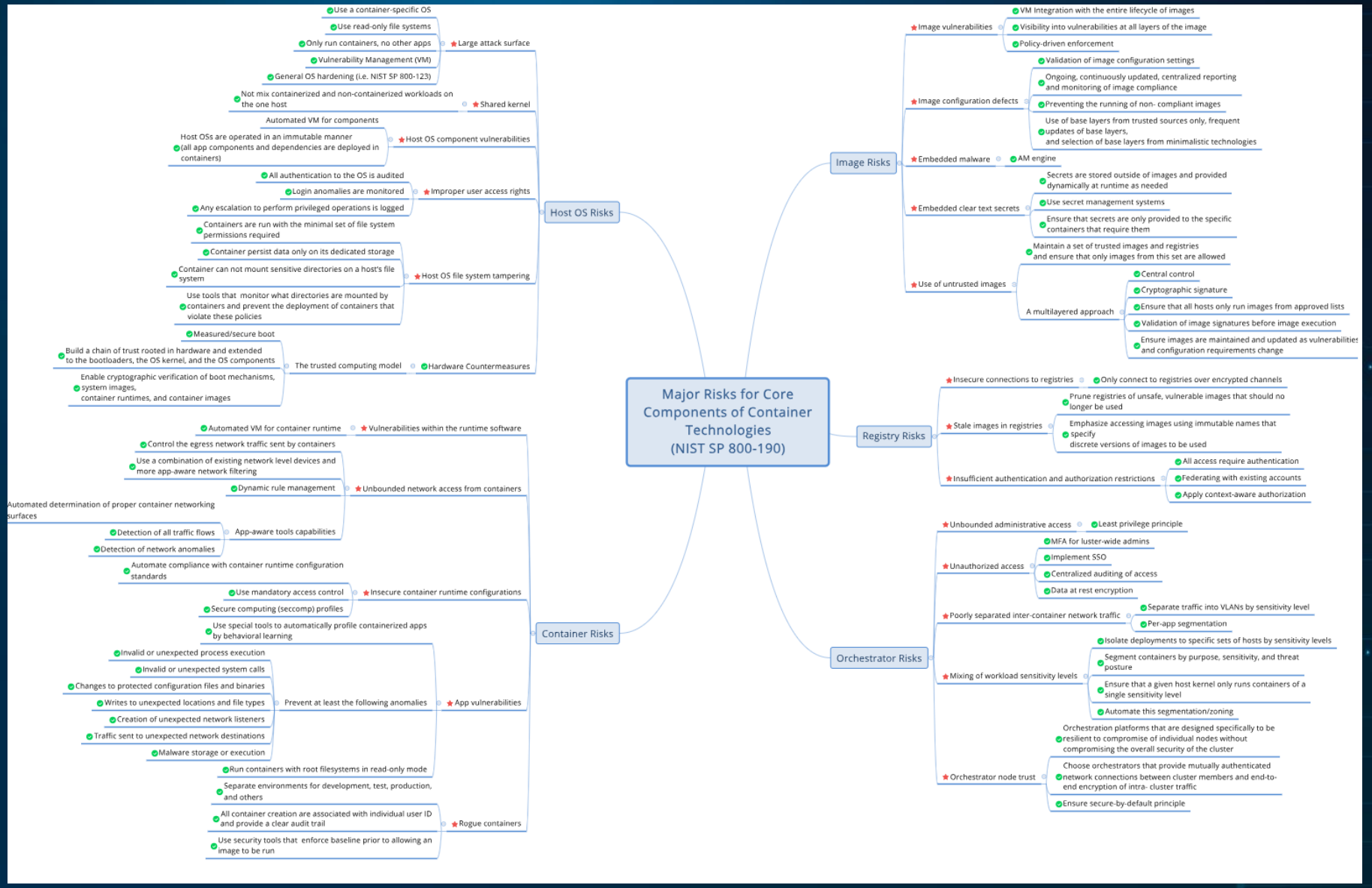
CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

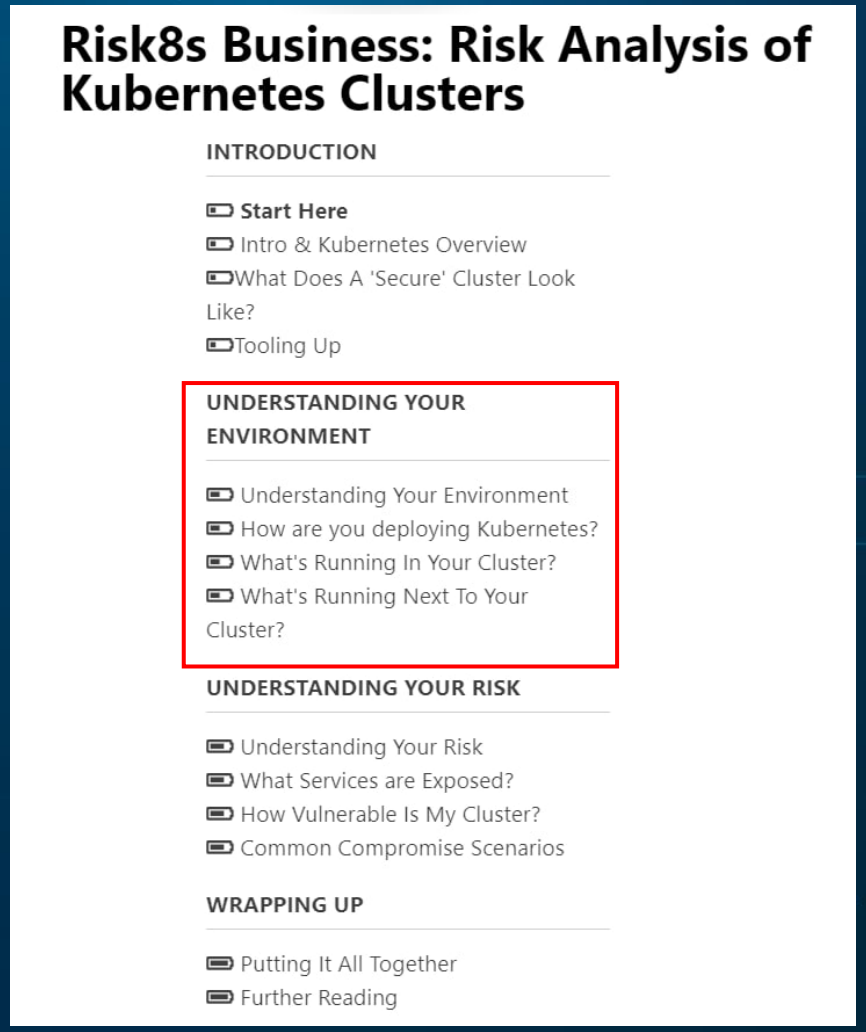
Вебинар Luntry. Соответствует ли ваш Kubernetes-кластер лучшим практикам?

LUNTRY
luntry.ru

NIST SP 800-190 Application Container Security Guide



Risk8s Business: Risk Analysis of Kubernetes Clusters



Источник

Взгляд Luntry

База на базе Luntry

База на базе Luntry

- **Актуальные версии**

База на базе Luntry

База на базе Luntry

База на базе Luntry

База на базе Luntry

База на базе Luntry

База на базе Luntry

Еще шаг вперед вместе с Luntry

И так далее вместе с Luntry

Итог

1. Понимайте свое окружение – полная инвентаризация.
2. Комплексный подход.
3. Приоритезируйте с учетом вашей модели угроз, поверхности атаки и моделей нарушителя.

Спасибо за внимание!

Дмитрий Евдокимов
Founder&CTO


Email: de@luntry.ru


Twitter: @evdokimovds

@Qu3b3c


Channel: @k8security


Site: www.luntry.ru

Андрей Ганюшкин
Коммерческий директор

Email: avg@luntry.ru

k8security luntrysolution